Downtime Costs How Much? Calculating the Business Value of Disaster Recovery

August, 2014

Introduction

As an IT professional, you will experience a system failure, outage, or complete site disaster. It's inevitable, and your organization probably already has some sort of disaster recovery (DR) plan in place.

Most days, you probably don't even think about DR. You focus on projects that streamline processes, decrease costs and give you some good visibility. DR is rarely considered strategic to the business. But when that disaster happens and you need to quickly restore your company's data and IT services, an ineffective DR plan can pose a serious threat to the company as a whole. And for you, it can mean the difference between being seen as a hero to the C-suite, or finding yourself in a job interview somewhere else.

Take, for instance, the Orleans Parish in New Orleans. As you can probably imagine given the location in an area prone to natural disasters, a DR plan was rightfully in place. However, when two servers that held the parish's conveyance and mortgage records dating back to the 1980s crashed simultaneously, their DR plan came up short.

An ineffective DR plan can mean the difference between being seen as a hero to the C-suite, or finding yourself in a job interview.

The Times-Picayune newspaper reported on the incident, saying that, "Without a complete and verified database of both conveyance and mortgage records, title companies can't be sure that a person trying to sell a property truly owns it free and clear. And the mortgage record database, which is separate from the one for conveyance records, is still missing about 100,000 documents."[1]

A bout of finger-pointing ensued. The parish's IT staff had thought it was backing up the parish's data using a cloud backup / disaster-recovery-as-a-service (DRaaS) provider. But neither the IT staff nor the service provider was aware that the data hadn't been backed up for months. What data had been backed up had passed its 30-day retention policy and was deleted.

In baseball, it's like two outfielders giving up on a fly ball because each player thinks the other will make the catch. The ball just drops to the ground with a thud and rests at both players' feet.

No doubt personnel at both the Orleans Parish IT department and the service provider found themselves scrambling to update their resumes.

What happened in Orleans Parish illustrates a situation that is all too common and yet completely avoidable. Effective disaster planning ensures that your business is adequately prepared to continue functioning in the wake of events that would otherwise be catastrophic. The purpose of this e-book is to put you on the path to developing an effective disaster recovery plan that will be seen as a strategic tool to your company's success.

2014 Dell. All rights reserved. | Share:

Expectations vs. Reality

As an IT professional it is certainly not surprising to hear that companies are more reliant on technology than ever before. With this increasing reliability on technology comes increasing expectation that it will, simply, work. And, increasingly — as shown by the 80% increase in number of days-per-week workers telecommute — from any location they choose to work.

End users have come to see IT as a service, like water or electricity. They expect that their company's data and applications will be available to them at all times, from any device. And they don't even think about it until it's no longer available.

Your customers' expectations have grown as well. For example, a customer trying to make a purchase through a company's website expects the transaction to go smoothly, whenever they're ready to buy and from whichever device they happen to be using.

Again, as an IT professional, this is hardly news. But what is surprising is the gap that exists between these expectations and the reality most companies face. While IT pros are doing all they can to meet these growing needs and challenges, an integral component of their mission — backup and disaster recovery — fail to receive the strategic focus and support they deserve. And, companies that do have DR plans in place often fall short in developing and executing the right DR plan.

Your mission, should you choose to accept it...

This misalignment between IT and the lines of business gives rise to a tremendous opportunity for you as an IT professional. You are already a jack of all trades — an expert in multiple domains. You are uniquely positioned to recognize the gaps and identify solutions. You can apply the tools and techniques needed to mitigate risks and position the company to thrive. It is IT professionals who can apply their knowledge in technology and think like business leaders that will advance and realize success in their careers.

It is IT professionals who can apply their knowledge in technology and think like business leaders that will advance and realize success in their careers.

There is a real opportunity here. You have the tools and know-how to bridge the gap and really stand out. This e-book series can help you organize your thoughts, ask the right questions and develop the right strategy to begin building a business-centric DR plan.

2014 Dell. All rights reserved. | Share:

Calculating the value of DR

DR is often neglected because it doesn't generate revenue or reduce costs. To take a more business-centric approach, you'll need to step outside your comfort zone and demonstrate the value that DR brings to the business. The number one way of doing this is to calculate how much a disaster would cost the company if one were to occur.

This can get complicated quickly since there are so many variables you can use. But simple arithmetic often does the trick, as long as the variables you use are realistic and the calculations stand up to scrutiny.

Cost of downtime	
Average yearly compensation per employee (salary + benefits)	$65,000
Total hours that F/T employees work per year	2,080 hours
Hourly compensation	$31 per hour
Number of employees unable to work due to the disaster	100 employees
Number of hours of downtime	8 hours
Total cost of downtime	**$24,800**

This example demonstrates the cost of a disaster that caused 8 hours of downtime during normal business hours.

Lost revenue	
Company's total yearly revenue	$10,000,000
Hours of operation	2,600 hours
Average revenue generated every hour	$3,846
Number of hours of downtime	100 employees
Total revenue lost	**$30,768**

You also would need to calculate your company's lost revenue.

Non-Recurring Costs (Per Disaster)	
Employee overtime / contractor pay to restore operations	$2,000
Vendor charges	N/A
Hardware repairs	$5,000
Total cost of downtime	**$7,000**

Be sure to add non-recurring costs associated with restoring operations, like hardware repairs, vendor charges (some less scrupulous vendors charge for the amount of data recovered), contractor pay, and employee overtime.

The total cost of eight hours of downtime in this particular example is **$62,568.** And if the downtime affects a customer-facing website or application, these numbers don't even begin to calculate the cost of customer frustration, a flood of calls to your customer support teams, or giving your customers an opportunity to consider alternatives. The outcome of your calculation will be different, but the key principles of how to calculate the value of DR are the same.

2014 Dell. All rights reserved. | Share:

Common terminology

There are related terms we commonly use when we talk to our IT colleagues, but there is often confusion about the actual meanings when you go outside of the data center, so it's best practice to clearly define what you are talking about. That way, everyone is on the same page.

Disaster recovery (DR) is the series of steps taken to recover IT services after a disruptive event using the tools and techniques at your disposal. For the purpose of this e-book, we are referring specifically to the recovery of applications, data, network, IP telephone systems, and all other technology necessary to conduct business.

Backup is a vital component of DR. It is the creation of point-in-time copies of your data. That data could be unstructured or structured, it could be file-, block-, or image-based. Each has its pros and cons.

Business continuity (BC), (or business resiliency,) is more expansive than disaster recovery because it not only includes the restoration of data and IT services, but also the processes and procedures taken to maintain business operations during a disaster.

High availability (HA) technologies are critical components that can help your business to continue to operate during a disaster. HA provides redundancy of production systems so that if one fails, another can quickly "fail over" and take its place. It does not protect against corruption. It's intended to fulfill an entirely different need and, therefore, should not be considered a substitute for a robust DR strategy.

It's important to note that virtualization and modern backup solutions are blurring the lines between DR and business continuity. For example, many organizations are leveraging the two technologies to create "virtual standby" systems. Ideal for your most mission-critical application servers, this method minimizes downtime and data loss by keeping standby virtual machines (VMs) at the ready. The standby VMs are continually updated; and in the event of a disaster, they can be rolled back to any point in time and temporarily assume the role of the production server. When the primary machine is restored, users are then able to fail back with all the changes that were sent to the standby VM.

To make business stakeholders aware of the urgency of disaster recovery is going to require a combination of technological prowess and business-leader thinking.

Conclusion

When you consider the stakes involved, it's clear that — despite not increasing top-line revenue or reducing cost — DR is absolutely essential to the business. To make other stakeholders aware of the urgency of DR is going to require the perfect combination of technological prowess and business-leader thinking. That's where you come in.

2014 Dell. All rights reserved. | Share:

© 2014 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.Dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.Dell.com
Refer to our Web site for regional and international office information.

Ebook-DowntimeCostsHowMuch-US-GM-24786

Nine Steps to Building a Business-Oriented Disaster Recovery Plan

September, 2014

Introduction

In our e-book, Downtime Costs How Much? Calculating the Business Value of Disaster Recovery, we talked about why disaster recovery (DR) is absolutely essential to the business, despite not increasing top-line revenue or reducing cost. We talked about how to calculate the value of DR and how it takes both technical know-how and business-like thinking to illustrate the importance of DR to the stakeholders who allocate the budgets. In this e-book, we start by highlight the top business-threatening data disasters, and then offer nine steps you can implement to build a business-oriented DR plan.

It's more likely that the next data-center disaster will be caused by something more mundane, like a power failure.

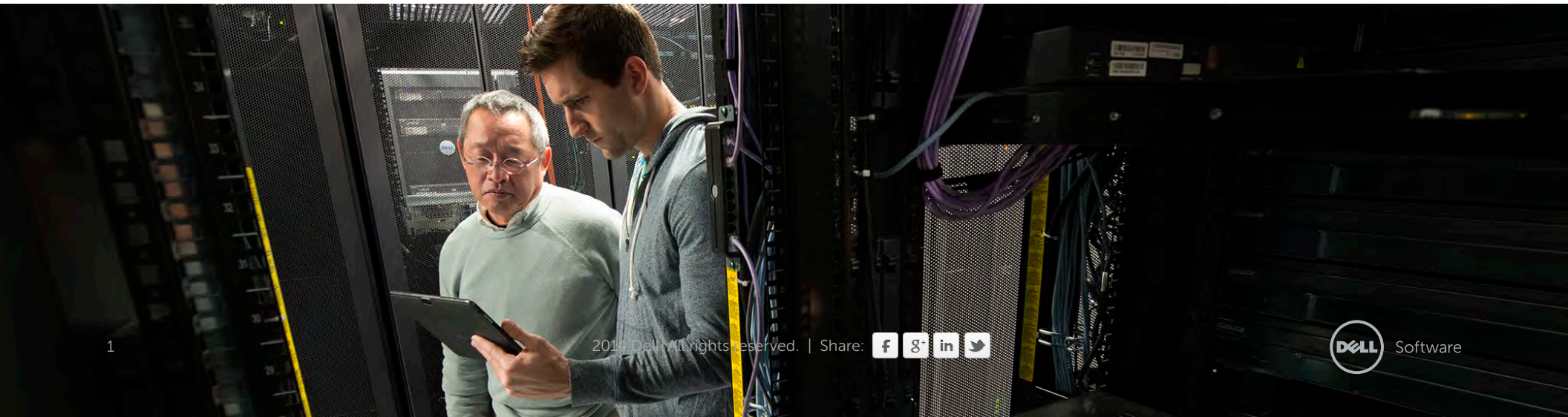
Getting on the same page

To begin, everyone needs to get on the same page with regard to the definitions and key assumptions. You have the opportunity to help others understand the nature and probability of the different disasters and what constitutes recovery. The meaning of disaster and recovery can vary — not only across the industry, but also within an organization.

Business managers, application owners, and IT admins likely have different ideas of what is considered an acceptable level of downtime and data loss. They probably don't agree on what systems are critical to the survival of the company.

Most people (outside of IT) consider a "disaster" to be a calamitous event — one that occurs suddenly and causes great loss of life, damage, or hardship. But within the world of IT, a disaster is any unexpected event that causes a substantial loss of service levels in critical business systems for an unacceptable period of time.

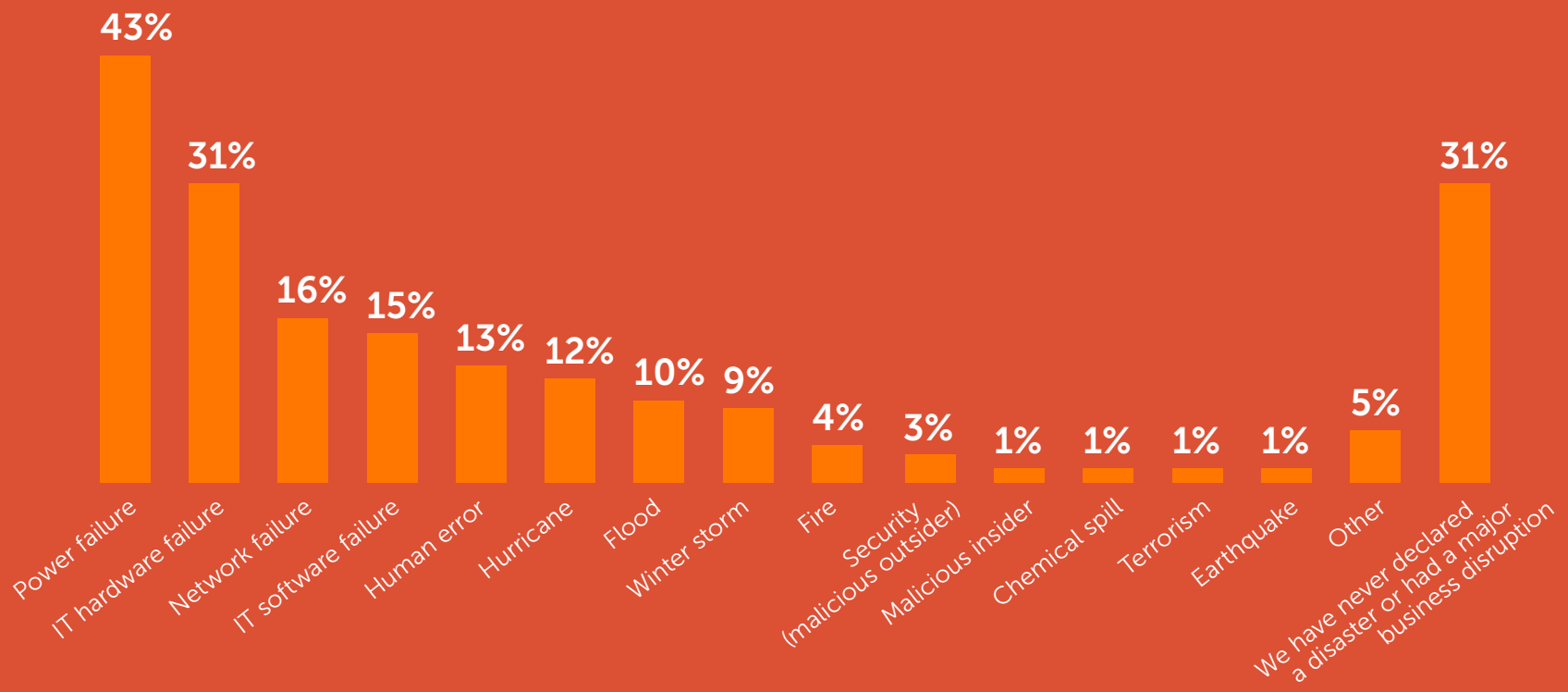
A disaster could be caused by something calamitous, yes. But statistically speaking, it's more likely that the next data-center disaster will be caused by something more mundane, like a power failure. It's important to make everyone in the organization aware of this fact.



2014 Dell. All rights reserved.

Top causes of downtime are mundane events, not disasters

What was the causes of your most significant disaster declarations or major business disruption?



Base: 94 global disaster recovery decision makers and influencers (multiple responses accepted)

Source: Forrester/Disaster Recovery Journal, November 2013 Global Disaster Recovery Preparedness Online Survey. Forrester Research, Inc. 109224

2014 Dell. All rights reserved. | Share:

The top business-threatening events aren't what you think

Human error

Human errors often cause systems to become logically corrupt or unusable. An accident as simple as an employee tripping on a cord can bring down an entire storage system.

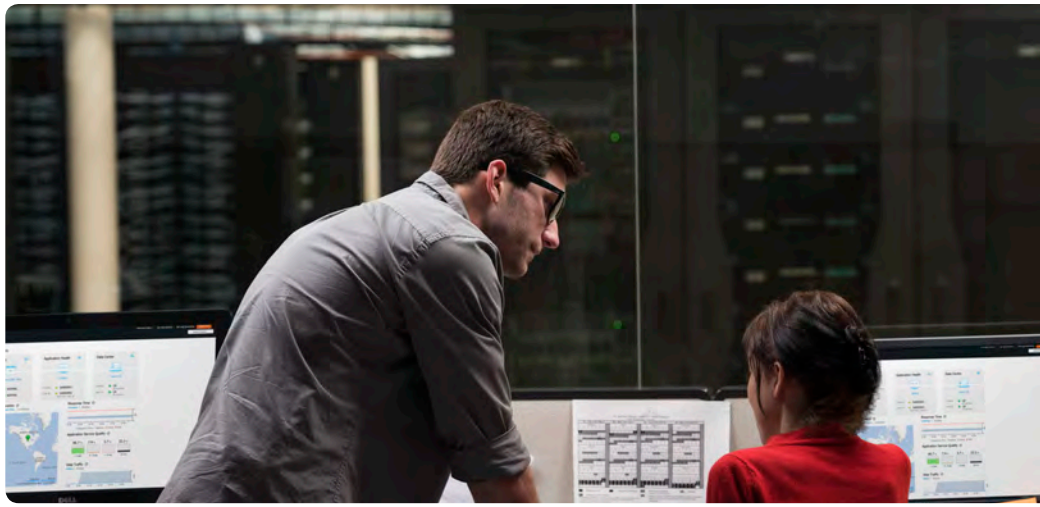
Malicious attack

While accidental human actions are common problems, intentional actions are increasingly common. Today, of course, organizations are even more aware of the possibility of malicious acts causing disasters. For example, disgruntled or former employees can attack and bring down IT systems, and so can viruses. An even more pressing concern of late is cyber-terrorism, especially threats against critical industries or government offices from groups or countries opposed to their actions or policies.

Data corruption

A data corruption outage occurs when a corrupt hardware or software component causes corrupt data to be read or written to the database. Data corruption takes many forms. It can be widespread or it can be localized. The impact of a data corruption outage will vary accordingly.

While accidental human actions are common problems, intentional actions are increasingly common.



Corruption in a single database block might affect few users, while corruption in a large portion of the database would make it essentially unusable. Most IT professionals have seen some form of data corruption in their careers, although organizations understandably tend not to publicize these problems. Such data corruption can be caused by hardware failures or human error.

Storage failures

A storage failure outage occurs when the storage holding some or all of the database contents becomes unavailable because it has shut down or is no longer accessible. Many companies have had complete storage failures — often caused unintentionally by pesky humans. For example, at one organization, someone stacked a set of disk drives against a wall, inadvertently turning off a switch and causing system failures — an issue that was difficult to track down.

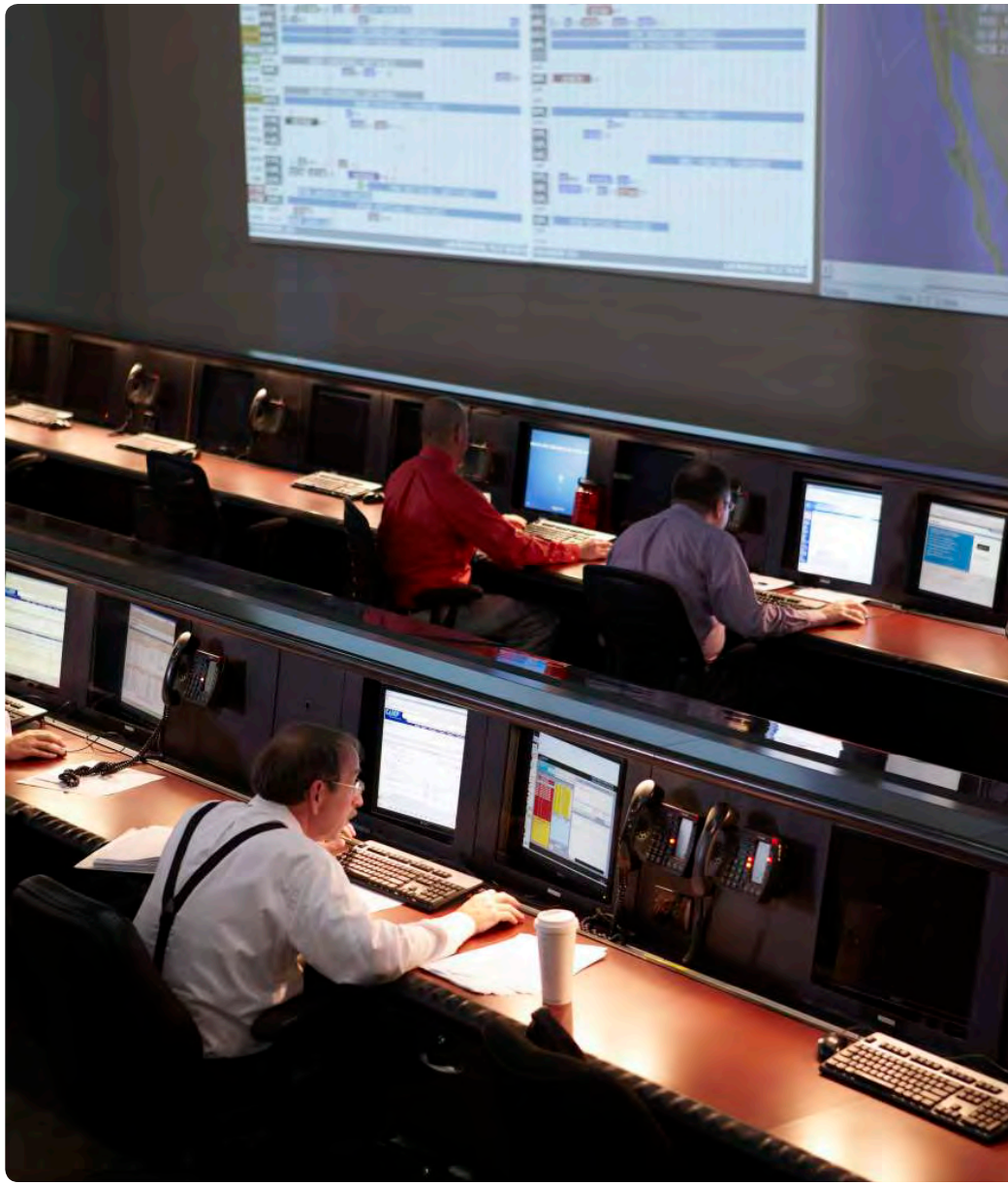
Another company that relied heavily on its storage area network (SAN) made the seemingly simple choice to lay carpet in its data center to reduce noise. When an authorized employee walked in to check the SAN and touched its racking bay, the static electricity discharge shorted the controller unit and the entire SAN went down. Without knowing that the cause of the problem was the electrostatic charge built up by walking on the carpet, the company put in a new controller. After it was up and running, someone else touched the rack again, and the new controller was also fried.

2014 Dell. All rights reserved. | Share:

Power and network failures

Power failures can seem mundane, yet they can have a crippling effect on the business. And they are cited as the number one culprit of downtime, according to the Forrester Research graphic shown on page 2. Web hosting provider DreamHost experienced this firsthand in 2013 when the power systems failed at its data center in Irvine, Calif. The incident created hours of downtime across two days and affected more than 350,000 customers.* It was a perfect storm: One of DreamHost's vendors had been performing unannounced maintenance on its UPS systems and the systems failed — resulting in a complete power outage. To make matters worse, the vendor's redundant power systems did not kick in.

Servers and storage often get all the attention in DR planning, but any business-centric DR plan should also include a redundant local area network (LAN) network infrastructure as well as steps on how to restore the LAN. Network failures are the third most common cause for unplanned downtime. The loss of a single network switch could quickly turn into a major, time-consuming outage for the organization.



Power failures can seem mundane, yet they can have a crippling effect on the business, and are cited as the number one culprit of downtime according to Forrester.

Natural disasters

Natural disasters like Hurricane Sandy and the 2011 earthquake and tsunami in Japan will be the types of disasters that will jump to the mind of your business colleagues when you mention disaster recovery, though they happen less frequently than IT-related failures.

Situations like these happen every day, with even the most experienced IT professionals on staff. Organizations must accept that disasters will happen, and build a sound recovery strategy to minimize their impact.

* news.dice.com/2013/03/21/power-outage-takes-down-dreamhost/

2014 Dell. All rights reserved. | Share:

Nine steps to building a business-oriented DR plan

Although IT disasters are unpredictable, recovery shouldn't be. In fact, recovery should be planned, predictable and controlled. The following steps will help you organize your thoughts, ask the right questions, develop the right strategy to build a DR plan that is closely aligned with your business.

1. Conduct an asset inventory

Disaster recovery planning should always start with an inventory of all your IT assets. This is necessary to untangle the complexity of your environment. Start by listing all the assets under IT management, including all servers, storage devices, applications, data, network switches, access points, and network appliances. Then map where each asset is physically located, which network it is on, and identify any dependencies. See example on Page 6, Table 1.

2. Perform a risk assessment

Once you have mapped out all your IT assets, networks, and their dependencies, go through each and list the internal and external threats to each of those assets. Imagine the worst case scenario — and be thorough. These threats could include natural disasters or mundane IT failures.

Next, include the probability that that event may happen and the impact it would likely have if that event were to occur. How will it affect the business if each scenario were to occur? This is also a good time to enlist the help of your business colleagues. Just remember to emphasize the fact that mundane events happen much more frequently than natural disasters. Move the conversation away from earthquakes and hurricanes and more toward higher probability that the location will experience a power outages or IT hardware failure. See example on Page 6, Table 2.

3. Define criticality of applications and data

Before you begin to build out your business-oriented DR plan, you'll need to classify your data and applications according to their criticality. Start by speaking to your business colleagues and support staff to determine the criticality of each application and data set.

Look for commonalities and group them according to criticality to your business, frequency of change, and retention policy. You do not want to apply a different technique to every individual application or dataset that you have. Grouping your data into classes with similar characteristics will allow you to implement a less complex strategy.

Classifying data in a vacuum based on assumptions may come back to haunt you. Be sure to involve other business managers and support staff in this exercise. You will undoubtedly have to make some trade-offs to limit the number of data classes you have. For medium-sized businesses, the number of classes should likely be between three and five. See example on Page 6, Table 3.

2014 Dell. All rights reserved. | Share:

Location	Server/VM	OS and hypervisor	Application	IP address	Disk allocated	Disk used	Dependencies
SFO-1	Orcl-001	RHEL 5.x	Oracle 11g	10.10.10.1	5 TB	1 TB	
	Exch-001	Win 2012 r2	Exchange 2013 (DAG1)	10.10.10.2	20 TB	7 TB	Exch-002
	Exch-002	Win 2012 r2	Exchange 2013 (DAG2)	10.10.10.3	20 TB	7 TB	Exch-001
	MOSS-001	Win 2012 r2	SharePoint 2010	10.10.10.4	10 TB	8 TB	SQL-01, SQL-02
	SQL-001	Win 2012 r2	SQL Server 2008	10.10.10.5	5 TB	3 TB	
	SQL-002	Win 2012 r2	SQL Server 2008	10.10.10.6	5 TB	2 TB	
	SQL-003	Win 2012 r2	SQL Server 2008	10.10.10.7	5 TB	2 TB	
	SQL-004	Win 2012 r2	SQL Server 2008	10.10.10.8	5 TB	2 TB	
	AD-001	Win 2012 r2	AD Domain Controller	10.10.10.9	3 TB	1 TB	

Table 1: An example of an inventory of one company's IT assets

Location	Assets	Threat (internal and external)	Probability	Impact
SFO-01	Orcl-001, Exch-001, SQL-001, SQL-002, SQL-003, SQL-004, SQL-005, FLS-001	Natural disaster - Earthquake	Low	High
		Network failure	Medium	Medium
		Power failure	High	High

Table 2: Risk assessment

Class	Description
Low impact	All data and systems that are needed to achieve the business' strategic objectives, but does not need to be immediately restored for the business to continue to operate.
Moderate impact	All data and systems that are important to the achieving business objectives. The business can operate but in a diminished state.
High impact	All data and systems that are critical to the business operations. Business comes to halt without the associated services.

Table 3: This example of a classification scheme includes three categories.

2014 Dell. All rights reserved. | Share:

4. Define recovery objectives

Different classes will have different recovery objectives. For instance, a critical ecommerce database may have very aggressive recovery objectives because the business simply can't afford to lose any transactions or be down for long. On the other hand, a legacy internal system may have less stringent recovery objectives (since the data doesn't change very often and it's less critical to get back online).

This is the step where many IT professionals fall short. Setting recovery objectives without consulting the business line managers is the number one cause for misalignment. It's imperative that you involve them in this process.

> Setting recovery objectives without consulting business line managers is the number one cause for misalignment.

Here is a sample list of questions you can ask your business colleagues:

- What applications and data does your department use?
- What is your tolerance for downtime for each?
- What is your tolerance for data loss for each?
- Are there times when these applications are not being used by employees, partners or customers?
- Would you ever need to restore data that is older than 90 days old? How about 6 months old? How about 1 year old?
- Are there any requirements (internal or external [i.e industry or regulatory]) for the organization to retain the data for a designated period of time?
- Are there any requirements (internal or external [i.e industry or regulatory]) that prevent us from moving the data from one geographical region to another?
- Are there any requirements (internal or external [i.e industry or regulatory]) with regard to security and encryption?

The key here is to understand business needs and provide a differentiated level of service availability based on business priority. Now that you have that information in hand, it needs to be translated into recovery objectives to be included in your DR plan. See Page 10, Table 4 for an example asset class breakdown.

Recovery time objective (RTO) — What is the acceptable time any of your data and production systems can be unavailable? This is your recovery time objective. To calculate the RTO for an application, consider how much revenue your organization would lose if the application went down for a given length of time.

For example, how much would you lose if your customer portal went down for an hour, or a day? How much cost would be incurred if none of your employees can work because email is down?

Calculating your RTO is necessary for determining the features you need in your backup systems and products. For example, if you have a very high RTO (say, more than four hours), you will probably have time to back up from tape, but if you have a very low RTO (such as just a few minutes), you need to use host-based replication or a disk-based backup with continuous data protection features.

Recovery point objective (RPO) — What is the acceptable amount of data your organization can afford to lose? That is your recovery point objective. If your organization has a high tolerance for data loss, your recovery point objective (RPO) can be high, from hours to days. If your business can't afford to lose any data, or very little, your RPO will be seconds.

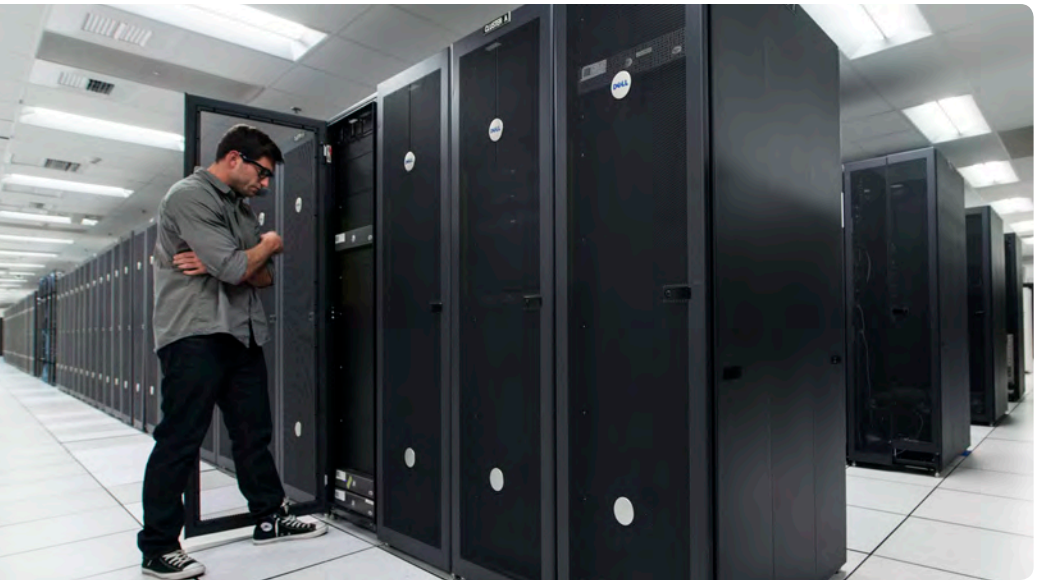
The RPO you set will determine the minimum frequency for backing up your data. If you can only afford to lose an hour's worth of data, you should back up the data at least every hour. That way, if an outage begins, for example, at 2:30 p.m., you can retrieve the 2:00 p.m. backup and meet the RPO requirement.

5. Determine the right tools and techniques

Once you have identified all your IT assets, mapped their dependencies, and grouped them together based on their criticality and recovery objectives, it's now time to choose what tools and techniques to use.

The good news is that a wide array of solutions is on the market today. Just make sure that what you choose offers the appropriate level of protection. Over-protection can cost the company needless money and introduce unnecessary complexity. (Complexity is the enemy of productivity and will likely increase the possibility for human error.) Under-protection can be equally bad since it will put important business functions at risk.

2014 Dell. All rights reserved. | Share:



For instance, nightly backups using traditional (file-based) methods are more than sufficient for low-impact data, but would be inappropriate for high-impact data and applications. A CDP solution is great for high-impact data and systems, but it can add overhead to production servers and storage costs.

Perhaps the most critical component of your DR plan is offsite protection. This should be used regardless of the type of backup method you choose. The method (be it tape vaulting service or replication to the cloud) should be commensurate to your recovery objectives. Make sure your data is sent to a location that is far enough away that it is not in the same geographic risk zone. Typically, this is at least 25 miles away from the primary location.

Finally, automate and streamline the recovery process as much as you can. In the event of a disaster, key IT staff may be unavailable. Automation also lessens the risk of human error.

Later in the e-book you'll find a deeper dive into the specific technologies on the market today.

Tip: David Shulman of Salomon Brothers once applied the Goldilocks principle to economics when he wrote a strategy piece entitled, "The Goldilocks Economy: Keeping the Bears at Bay". In this report, he was referring to an economy that was hot enough for profit growth, but cool enough to keep the Fed from hiking interest rates. This principle can also easily be applied to disaster recovery planning. The method you use should be just right for the classification of data that you are protecting. This obscure reference will no doubt elicit nods of approval in the board room.

Another high priority is something that is often overlooked as a best practice during a disaster recovery: establishing a "dial-tone" email system that enables all users to send and receive new emails during a power outage. The term dial-tone is used because even during power outages, phones often continue to work, and users really should be able to expect a similar level of dial-tone service for mission-critical communications like email. It may take a while to restore all of the email history for all of the users, but that is largely irrelevant to the pressing need to communicate in real time following a major outage or disaster. The dial-tone email service can also help relieve some of the pressure on the IT staff to get everything up and running as soon as possible.

Perhaps the most critical component of your DR plan is offsite protection.

6. Get stakeholder buy-in

Go beyond the walls of the data center and involve key stakeholders for all your business units (i.e. application owners and business managers). They need to be involved in the planning phase. And they should agree with you on the company's priorities and service level agreements (SLAs) your team will provide.

Also, consult your strategic partners and vendors to make sure you're getting the most out of your DR solution and/or services. When two servers failed at the Orleans Parish in New Orleans, causing the loss of critical conveyance and mortgage records dating back to the 1980s, IT staff hadn't been keeping in close contact with the parish's cloud backup / DRaaS provider. Similarly, when web hosting provider DreamHost had an outage, the company identified the source of the problem to the

2014 Dell. All rights reserved. | Share:

vendor that manages its data center. Be sure not to make that mistake and stay in close contact with any vendor you employ.

Once you have consulted all of the key stakeholders, enlist an executive-level sponsor who will get behind you and the project. The importance of collaboration, consensus and executive support to your DR plan's success cannot be emphasized enough.

7. Document and communicate your plan

In a disaster scenario, you need a documented strategy for how to get back to a working state. This document should be written for the people who will use it.

Communicate your plan. All too often, only one person in the organization really knows the whole picture, leaving the organization vulnerable if that one person is unavailable during a disaster. In addition, be sure to store your recovery strategy where it can be accessed during a disaster — not on public share in your Exchange folders. Ideally, it should be printed and posted in multiple locations.

8. Test and practice your DR plan

People often say, "Practice makes perfect." A better saying might be, "Practice makes progress." No organization ever gets to perfection with its DR plan, but practice will help you find and rectify problems in your plan, as well as enable you to execute it faster and more accurately. Make sure that everyone who has a role to play attends the practice sessions, even if you hold them, for example, on Saturdays.

You do not need to practice executing the full disaster recovery plan every time. It's perfectly acceptable to carve out pieces of your plan to test. See example on Page 10, Table 5.

9. Evaluate and update your plan

A DR plan should be a living document. It's especially important to regularly review your plan given the shifting sands of an ever-changing business environment. Tolerance for downtime and data loss may decline. Key personnel may go on leave or terminate their employment. IT might migrate to new hardware or operating systems. The company might acquire another company. Your plan needs to reflect the current state of the organization.

2014 Dell. All rights reserved. | Share:

Classification	Application	Server/VM	RTO	RPO
Low impact	Filesystem	FLS-001	24 hrs	24 hrs
Moderate impact	SharePoint, Active Directory	MOSS-001, AD-001, SQL-001, SQL-002	12 hrs	12 hrs
High impact	Exchange, Oracle	Exch-001, Orcl-001	1 hr	10 min

Table 4: Document the RTO and RPO for each asset class

Class	Description	Frequency
Walk-thru exercise	Review the layout on contents of your DR plan	As often as necessary to familiarize response teams and individuals with a documented plan or changes to a plan
Tabletop exercise	Using a scenario, discuss the response and recovery activities of a documented plan	At least 4 times per year, or any time a change is made to the business or IT operating environment.
Component exercise	Physically exercise a component of a DR plan (e.g. testing automated communications services or work-from-home capabilities together with IT or partner capabilities)	At least twice per year or when a change is made to the business or IT operating environment
Full-scale simulation	Using a scenario, carry out the response and recovery activities of a DR plan the entire organization	At least once or twice per year or when a change is made to the business or IT operating environment

Table 5: Here is an example of different test types with their frequency

2014 Dell. All rights reserved. | Share:

DR tools and techniques

Choosing the right approach (or approaches, as may be the case) to protect business-critical data and applications can be daunting. After all, there are many more solutions on the market today than there was just a few years ago. And some of these new solutions blur the lines between high availability and disaster recovery.

The best way to choose a solution to successfully recover after a disaster is, again, to think like a business leader. Choose a solution that offers the best value — one that doesn't cost the company needless money, introduce unnecessary complexity or put important business functions at risk.

Some may try to convince you that traditional backup (aka file-level) methods are outdated. However, file-level backups often form the foundation for a comprehensive data protection and disaster recovery plan. With these solutions, you select the files, folders, and databases that you'd like to back up. The backup solution scans the file system and makes a copy of each data set to a different destination. This is performed on regular schedules, typically once a day.

Continuous data protection (CDP) solutions have become more popular since they offer impressive backup and recovery speeds.

If traditional backup meets your recovery objectives, go with it. Don't succumb to marketing hype. That approach is absolutely the right business decision. Just be sure to choose a solution that offers a wide range of support for various applications, but also doesn't complicate — and therefore jeopardize — the recovery process.

Continuous data protection (CDP) solutions have become more popular since they offer impressive backup and recovery speeds as well as very granular recovery points (from seconds to minutes). A CDP solution works at the sub-file level, watching all of the new/changed blocks of data and only capturing those blocks.

Image-level backup (aka bare metal restore or BMR) is a data recovery method that enables you to quickly get a complete system running again after a disaster — even if the environment has no functioning operating system. A BMR solution not only backs up the data, but also the operating system and the application and configuration settings, Therefore, you can quickly rebuild a server, including its operating system, network and system settings, application binaries, disk partitions and data.

A new generation of backup solutions is emerging. These modern backup solutions periodically create restore points using a snapshot and volume filter device driver to track disk changes. This enables the solution to perform a restore of a failed server or VM in minutes.

Backups are also application-consistent, meaning the buffers flushed, files closed etc. so that the integrity of the data is protected and there will be no issues during a restore. To ensure recoverability, one solution even validates its latest backup by completing an integrity check for any sort of corruption and mounting the backup copy of the database.

Many companies are complementing their backups with array-based snapshots because they are low-impact, near-instantaneous, space-efficient, and allow them to quickly recover entire volumes of data or at the granular level. Once a base snapshot is taken of any data written to a volume, only incremental changes are captured in subsequent snapshots. This not only saves disk space, but speeds local recovery.

Users can create many snapshots without setting aside extra disk space, and those snapshots can all be scheduled at very short intervals (depending on your RPO). In rare cases, these snapshots are also application-consistent — meaning that all open transactions have been committed, buffers have been flushed, files have been closed, and the application is ready for the snapshot to occur.

Tip: If you are creating array-based snapshots, make sure to conduct a test failover from that snapshot so you can validate application-consistency.

Snapshots can cause complexity because they operate outside your normal backup operations. However, some backup applications on the market today complement

2014 Dell. All rights reserved. | Share:

array-based snapshots, allowing users to generate, schedule and recover snapshots through the same user interface. This allows you to simplify and centralize management.

Some backup applications also support single-file restores. They do this by recording checkpoints throughout the backup and saving the file history information on a per-file basis. To restore a single file, the backup application only has to read a small part of the backup data to find and restore the requested file(s).

Regardless of the method you choose, it is essential that the backup data be replicated to secondary location or the cloud. Some storage solutions will only replicate the incremental changes following initial site synchronization. This approach not only reduces hardware costs, but minimizes bandwidth requirements and accelerates recovery in the event of a disaster. Virtualization is also a great enabler, allowing you to maintain standby VMs at the secondary location — ready for deployment when disaster strikes.

Vendor considerations

Now that you've got a plan for how to build your business-centric DR plan, you may find you need to either completely replace or complement your existing solutions. You'll find dozens of products on the market from many different vendors, so it may be difficult to distinguish between them and ultimately make that decision on who you want as your partner.

Look for a vendor with solutions that are easy to acquire and deploy. Vendors have increasingly become more flexible when it comes to licensing. Choose a licensing model that will accommodate growth. Buying backup by component is a good idea if you aren't planning to add a lot of servers and applications. Alternatively, buying backup by capacity may not make sense when you have a few NAS filers with petabytes of data to protect.

Also, look for opportunities to buy a bundle of solutions at a discount. Finally, be on the lookout for any "gotchas." We mentioned earlier that some vendors charge for the amount of data you recover!

Purpose-built backup appliances (PBBAs) are gaining in popularity because of their ease of deployment. These solutions include backup software, hardware and storage, making it very easy to get started.

Deduplication appliances can help when you can't afford to completely rip and replace your existing backup solution. Some offer "accelerator" technology, which can greatly improve backup and restore performance as well as reduce the backup traffic over your network. They may also include replication capabilities, so you can safely and efficiently send your backup data to your DR site.

Regardless of the vendor you choose, ensure that the solution strikes the right balance between capabilities and manageability. Some solutions on the market today include a lot of bells and whistles, but have an overwhelming amount of options for scheduling, tracking, data streaming options and require admins to define every minute detail of the backup process. This can introduce the possibility for human error. The right solution will offer enterprise-grade capabilities and an intuitive user experience.

Support and maintenance is also a key consideration. Look for a vendor that has a proven track record of supporting the latest applications and operating system releases (i.e. Oracle 12c, Windows Server 2012 R2, etc).

Lastly, choose a vendor that is able to offer the lowest total cost of ownership. That includes not only license fees, but also maintenance renewal fees and professional service fees required for upgrades and tune-ups, as well as all of the hardware costs required to run the backup system. You'd be surprised at how quickly these add up.

Conclusion

There is misalignment between what the business expects and what IT can actually deliver — especially when it comes to disaster recovery. Following these nine steps can help you organize your thoughts, ask the right questions and develop the right strategy to begin taking a more business-centric approach to disaster recovery planning . These steps can also help you become an IT hero, or possibly even get you a seat in the C-suite.

2014 Dell. All rights reserved. | Share:

© 2014 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.Dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.Dell.com
Refer to our Web site for regional and international office information.

Ebook-9StepstoBuildingBusinessOrientedDisasterRecoveryPlan-US-GM-24786